DOE and TrueArc meeting, December 13, 2001

The representatives from TrueArc were Russ Stalters, President and Chief Operating Officer (COO); Tim Shinkle, Chief Technology Officer (CTO) and Dave Warner, Director of Sales.

The DOE representatives included John Staley, Patrick Robert, and Bill Few (Cyber Security); Betty Beavers, Mary Milton-Rawlings (EH); Chris Squiers and Tom Lombardo (Host/CMSi/FE); Jay Blewett, Gaynell Simmons, Collin Batchlor, and Lorretta Bryant (CIO). By telecon, Kim Wandersee, Mark Oliver and Frank Cicchetto (EH).

After the introduction of the DOE representatives and a brief description of the purpose of the meeting, Russ began by explaining that he felt the underlying cause of the problem was a misunderstanding of how ForeMost works. He asked Tim to do a quick overview of the ForeMost architecture to be sure everyone was on the same page and to illustrate how its security functionality works.

Tim explained that ForeMost is based on a three-tiered architecture. The top tier sits on the user's desktop. The middle tier contains ForeMost Enterprise and is on the server. The third tier is the SQL or Oracle database and the document server. Only Enterprise (middle tier) communicates with the third tier. Records are not stored on the user's desktop, in the second tier, or the database but on the document server.

No user ever communicates directly with the database or the document server. The user accesses the ForeMost Enterprise through Distributed Compound Object Model (DCOM). The application opens a communications pool with the database and document server through one of the established accounts. This account queries the database and brings back the documents requested by the user. The end user has no direct access to the metadata database in SQL or Oracle or to the document server.

The document database has to be on an NT/2000 server. The password is not hard-coded, but it does have a default. TrueArc has the code that will allow the password to be changed. TrueArc will provide DOE with the tool to change the password.

ForeMost relies on Microsoft security. The security in ForeMost is only as good as your network's security in that it is based on the network security.

The user must be validated by the middle tier in order to get into the ForeMost Enterprise. Users are validated through ODBC. Only an authenticated domain user gets into the system.

It was asked if you could have a separate account from the network. You can require users to sign into Foremost separately from the LAN and not have a "trust" relationship where signing on the network gives you access to Foremost Enterprise.

When doing a search, the user only goes to the middle layer. When request to view a document, the request goes to the middle layer and then the middle tier then asks the document server for it. The application uses RPSC to communicate with the document server and ODBC to the document sever.

The Access Control List (ACL) is stored in the database. The account password is encrypted and cannot be reverse-engineered. The account system names cannot be changed, but the passwords can be changed. TrueArc is willing to look into the possibility of adding a feature to the application that will allow the account names to be changed. User names can be deleted, and new names created.

The documents are not cached in Foremost Enterprise after retrieval in response to a request. The link is cached. Data is the only thing that is cached in the middle tier. Once the information in the cache is no longer accessed, it is dumped after a specific time period.

TrueArc is going to verify that any ASCII character, other than the semicoln (;), can be part of the password. They will check and provide the information to DOE. They were certain that the limit was 8 characters. DOE promised to provide a copy of DOE's policy on passwords to TrueArc.

The question was asked about the capability of putting a banner warning for users regarding the types of documents that should not go into ForeMost. ForeMost does not support the use of banner warnings. However, the middle Tier API is available to customize the front-end screens as part of the Record Declaration screen..

Cannot reassign the authorities in the hard-coded accounts.

It is possible to turn on auditing for all functionality. Foremost depends on SQL or Oracle to do performance monitoring. The auditing results are put in a table in the database and can do reports based on the table. It is also possible to write it out to a flat file.

They do not have a tool for seeing what is in the middle tier cache. They do have a tool to flush the cache based on size limits.

TrueArc is looking at users authentication to validate that the record being viewed is the same as the one filed. One application, Authentidate, is almost a plug and play addition to Foremost.

It was asked if there is a way to implement ForeMost where it will be secured.

DOE has 20,000 licenses for Entrust (version 5 not 6) and are using it in a pilot.

Like to see more open product with minimum being x.509 compliant.

DOE will develop a section for the records management training that details what goes into the system, what does not and what policies are for electronic record. Russ suggested that DOE might want to develop two approved configurations for other DOE offices to use if they choose to implement Foremost. There would be one configuration for Oracle and one for SQL.

TrueArc promised answers to DOE's question by the next day. They also planned on sending an email that summarized the questions by COB today.